# Curso Superior de Tecnologia em Redes de Computadores
# Projeto Integrador II

## 1º Seminário de Andamento

Tiago Pasa
tiagopasa@hotmail.com

# IDS – Sistema de Detecção de Intrusão

Sistema de Detecção de Intrusão - IDS

Tiago Pasa

# Sumário

- Introdução
- Objetivos
  - Geral
  - Específicos
- Projeto
  - Situação atual
  - Próximos passos
- Cronograma
- Referências Bibliográficas
- Wiki

# Introdução

**Por que implementar um IDS?**

- Crescimento contínuo de incidentes relacionados à segurança da informação;
- Detectar varreduras de portas e tentativas de acesso;
- Manter a segurança, integridade e confidencialidade das informações;
- Identificar acessos externos e internos não autorizados;
- Monitoramento constante da rede e servidores que proveem serviços diversos.

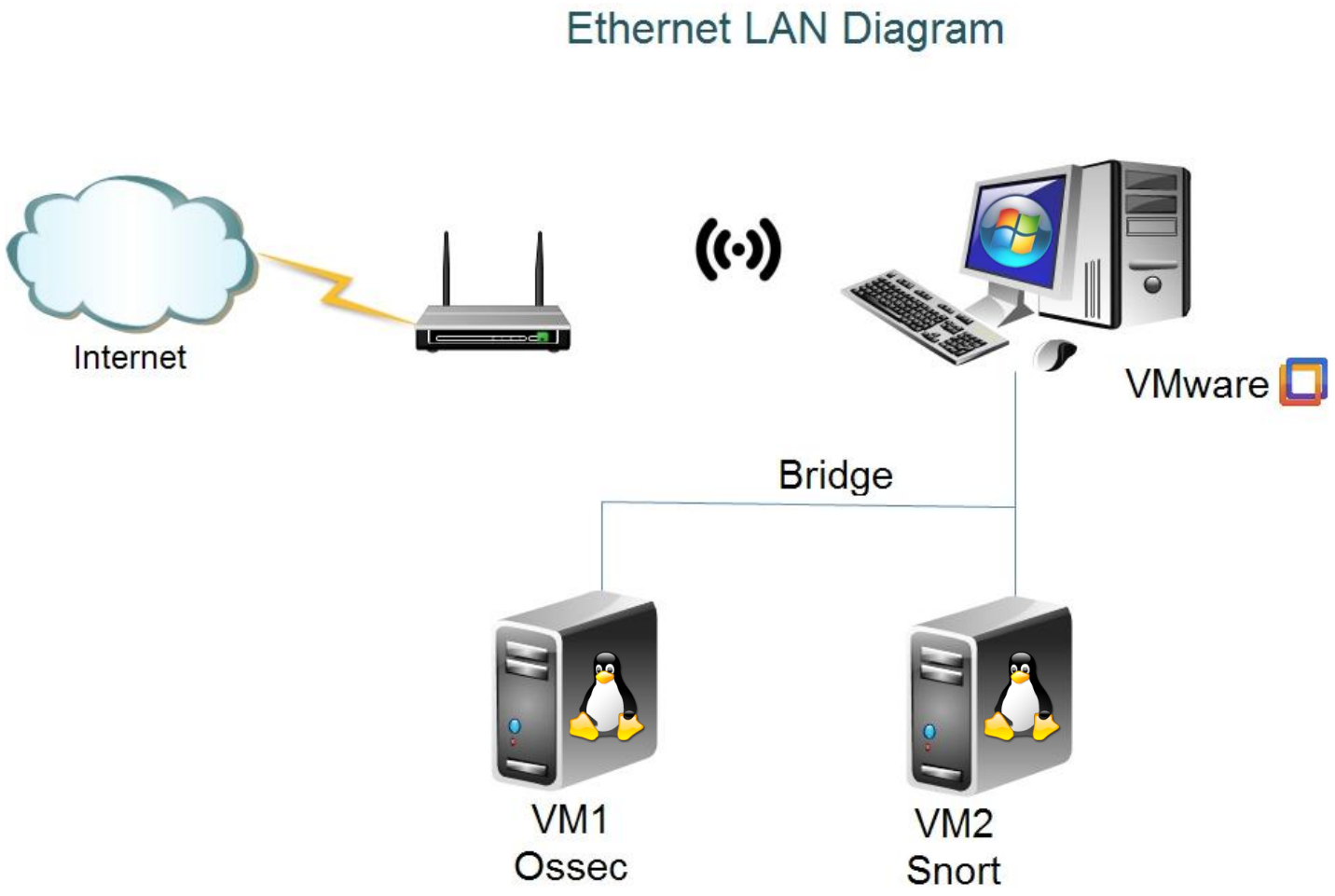
# Objetivos

- Objetivo Geral:
  - Testar software livre de detecção de intrusão em sistema operacional Linux

- Objetivos Específicos:

  - Pesquisar soluções livres;
  - Instalar ferramentas de detecção;
  - Realizar testes e comparações;
  - Realizar a documentação do processo.

# Situação Atual



# Situação Atual

- Máquinas virtuais com Linux, com os respectivos sistemas:
- **OSSEC** (HIDS - Host-based Intrusion Detection System);
- **Snort** (IDS/IPS - Network intrusion prevention and detection system).

# Situação Atual

- **OSSEC** (HIDS - Host-based Intrusion Detection System)
  - Open source;
  - Baseado em host;
  - Pode trabalhar como cliente/servidor
  - Capaz de monitorar integridade de arquivos, detectar rootkits, resposta automática de incidentes.
  - Plataformas Linux, Solaris, AIX, HP-UX, BSD, Windows, MacOS X e Vmware ESX.

# Situação Atual

- **Snort** (IDS/IPS - Network intrusion prevention and detection system).
  - Open source;
  - Baseado em rede;
  - Capaz de detectar em tempo real quando um ataque está sendo realizado na rede;
  - Plataformas Linux,BSD, Windows, MacOS X.

# Próximos Passos

- Configurações detalhadas dos IDS;
- Interface gráfica para análise de logs;
- Testes de funcionamento;
- Simulações.

# Próximos Passos

- **Simulações:**
  - **IDSWakeup** (False positive generator);
  - **Ftester** (Firewall Tester and IDS Testing tool);
  - **Nessus** (Vulnerability Scanner);
  - **OpenVAS** (Vulnerability Scanner).

# Cronograma

| | Março | Abril | Maio | Junho | Julho |
|---|---|---|---|---|---|
| Pesquisa de soluções livres | X | X | | | |
| Instalar ferramentas de detecção | X | X | X | | |
| Realização de testes e comparações | | X | X | X | X |
| Realizar a documentação do processo | | X | X | X | X |
| Escrita do artigo | | X | X | X | X |

# Referências Bibliográficas


- Ossec (2014). Disponível em: http://www.ossec.net/. Acesso em: 18 março 2014.
- Snort (2014). Disponível em: http://www.snort.org/. Acesso em: 18 março 2014.
- IDSWakeup (2014). Disponível em: http://www.hsc.fr/. Acesso em: 20 abril 2014.
- FTester (2014). Disponível em: http:// www.inversepath.com /. Acesso em: 20 abril 2014.
- Nessus (2014). Disponível em: http:// www.tenable.com /. Acesso em: 20 abril 2014.
- OpenVAS (2014). Disponível em: http:// www.openvas.org /. Acesso em: 20 abril 2014.
- Moraes, Alexandre Fernandes de. Segurança em Redes: Fundamentos. Editora Érica Ltda, 2010. ISBN 978-85-365-0325-7.
- Nakamura, Emílio Tissato. Segurança de Redes em ambientes Cooperativos. Novatec Editora, 2007. ISBN 978-85-7522-136-5.
- Diógenes, Yuri. Mauser, Daniel. Certificação Security+. Novaterra Editora e Distribuidora Ltda. ISBN 978-8561893-03-3.

# Wiki

- Projeto Integrador II – Projeto 03 (Externo)
- Projeto Integrador II – Projeto 03 (Interno)